

HN



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/668,610	09/22/2000	Carl M. Ellison	042390.P8104X	2283

7590 01/04/2005

Thinh V Nguyen  
Blakely Sokoloff Taylor & Zafman LLP  
7th Floor  
12400 Wilshire Boulevard  
Los Angeles, CA 90025

EXAMINER

ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center"><b>Office Action Summary</b></p>	<b>Application No.</b> 09/668,610	<b>Applicant(s)</b> ELLISON ET AL.	
	<b>Examiner</b> Kaveh Abrishamkar	<b>Art Unit</b> 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 23 July 2004.  
 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.  
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-8, 10-20, 22-32-34-44, 46-48 is/are pending in the application.  
     4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
 6) ☒ Claim(s) 1-8, 10-20, 22-32-34-44, 46-48 is/are rejected.  
 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
     a) ☐ All    b) ☐ Some \*    c) ☐ None of:  
         1. ☐ Certified copies of the priority documents have been received.  
         2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
         3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |  |
|---|--|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)<br>2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)<br>3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>04/05/2002</u> . | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____.<br>5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)<br>6) <input type="checkbox"/> Other: _____. |
|---|--|

## **DETAILED ACTION**

### ***Response to Amendment***

1. This Office action is in response to the amendment filed on July 23, 2004. The original application contained claims 1 – 48. Per the received amendment, claims 9, 21, 33, and 45 have been cancelled, and claims 1, 3, 10, 13, 14, 15, 22, 25, 27, 34, 39, and 46 have been amended. Presently pending claims are 1-8, 10-20, 22-32, 34-44, 46-48.

### ***Information Disclosure Statement***

2. An initialed and dated copy of Applicant's IDS form 1449, submitted April 5, 2002, is attached to this Office action.

### ***Response to Arguments***

3. Applicant's arguments, filed on July 23, 2004, have been fully considered but they are not considered persuasive because of the following reasons:

Regarding currently amended independent claims 1, 13, 25, and 37, the applicant argues that the cited prior art does not disclose "encrypting a value while operating in isolated execution mode" and/or "decrypting an encrypted value while operating in isolated execution mode." The applicant argues that these actions are not

Art Unit: 2131

performed, and also that an "isolated execution mode" is not disclosed in the cited prior art. These arguments are not found persuasive in view of the cited prior art England et al. (U.S. Patent 6,327,6552). The "isolated execution mode" disclosed in the claims, is interpreted as a mode in which other applications or other unauthorized areas of memory cannot access. England discloses a segment of memory (DRMOS) that prohibits the use of certain programs, prevents tampering, provides a secure storage space, and can prohibit all access when a trusted application is running (executing) (column 15 line 62 – column 16 line 67). The function of preventing access to a memory while a certain application is running can be interpreted as "isolated execution mode" because access is prohibited while the trusted application is running in the DRMOS. Further, the applicant argues that the operations of encrypting or decrypting a value while operating in an isolated execution mode are not disclosed in the cited prior art. England teaches that the "DRMOS can encrypt the content and similar protected information" (column 16 lines 23 – 31) and further can store and use keys, which are kept separate from other operating systems or software, for "secure storage and retrieval of protected information" (column 16 lines 50 – 60). The "retrieval of protected information" is a decryption operation.

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the subject matter "encrypting a value while operating in isolated execution mode" and/or "decrypting an encrypted value while operating in isolated execution mode" broadly recited in the amended independent claims 1, 13, 25, and 37. The dependent claims 2-8, 10-12, 14-20, 22-24, 26-32, 34-36, 44, 46-48 are rejected at least

Art Unit: 2131

by virtue of their dependency on the independent claims and by other reason set forth in this office action.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6, 10-18, 22-30, 34-42, and 46-48 rejected under 35 U.S.C. 102(e) as being anticipated by England et al. (U.S. Patent 6,327,652).

Regarding claim 1, England discloses:

An apparatus comprising:

a key generator to generate an operating system nub key (OSNK) unique to an operating system (OS) nub, the OS nub being part of an operating system running on a secure platform (Figure 8 item 801, column 7 line 45-61, column 17 lines 1-15); and

a usage protector coupled to the key generator to protect usage of a subset of a software environment using the OSNK (column 17 line 1 – column 18 line 13);

wherein the usage protector performs at least one operation selected from the group consisting of:

encrypting a value while operating in isolated execution mode (column 15 line 61 – column 16 line 67); and

decrypting an encrypted value while operating in isolated execution mode (column 15 line 61 – column 16 line 67).

England discloses an apparatus that uses an Operating System (OS) key to secure access to an operating system operating in a secure mode. Furthermore, England describes that “an unrelated operating system cannot gain access to the encrypted data” (column 17 lines 54-58) because of the requirement of the OS key.

Regarding claim 13, England discloses:

A method comprising:

generating an operating system nub key (OSNK) unique to an operating system (OS) nub, the OS nub being part of an operating system to run in a software environment on a secure platform (Figure 8 item 801, column 7 line 45-61, column 17 lines 1-15); and

protecting usage of a subset of the software environment using the OSNK (column 17 line 1 – column 18 line 13);

wherein the operation of protecting usage of a subset of a software environment comprises at least one operation selected from the group consisting of:

encrypting a value while operating in isolated execution mode (column 15 line 61 – column 16 line 67); and

decrypting an encrypted value while operating in isolated execution mode  
(column 15 line 61 – column 16 line 67).

England discloses an apparatus that uses an Operating System (OS) key to secure access to an operating system operating in a secure mode. Furthermore, England describes that “an unrelated operating system cannot gain access to the encrypted data” (column 17 lines 54-58) because of the requirement of the OS key.

Regarding claim 25, England discloses:

A computer program comprising:

a computer usable medium having computer program code embodied therein,  
the computer program product having:

computer readable program code to generate an operating system nub key  
(OSNK) unique to an operating system (OS) nub, the OS nub being part of an operating system to run in a software environment on a secure platform (Figure 8 item 801, column 7 line 45-61, column 17 lines 1-15); and

computer readable program code for protecting usage of a subset of the software environment using the OSNK (column 17 line 1 – column 18 line 13);

wherein the operation of protecting usage of a subset of the software environment comprises at least one operation selected from the group consisting of:

encrypting a value while operating in isolated execution mode (column 15 line 61 – column 16 line 67); and

decrypting an encrypted value while operating in isolated execution mode  
(column 15 line 61 – column 16 line 67).

England discloses an apparatus that uses an Operating System (OS) key to secure access to an operating system operating in a secure mode. Furthermore, England describes that “an unrelated operating system cannot gain access to the encrypted data” (column 17 lines 54-58) because of the requirement of the OS key.

Regarding claim 37, England discloses:

A system to provide a secure platform, the system comprising:  
a processor (Fig 1B item 160, column 7 line 44-50);  
a storage device coupled to the processor, the storage storing a subset of a software environment to run on the secure platform (Fig 1B item 184); and  
a usage protector comprising:  
a key generator to generate a operating system nub key (OSNK) unique to an operating system (OS) nub, the operating system nub being part of the software environment (Figure 8 item 801, column 7 line 45-61, column 17 lines 1-15); and  
a usage protector coupled to the key generator to protect usage of a subset of the software environment using the OSNK (column 17 line 1 – column 18 line 13);  
wherein the operation of protecting usage of a subset of the software environment comprises at least one operation selected from the group consisting of:



encrypting a value while operating in isolated execution mode (column 15 line 61 – column 16 line 67); and

decrypting an encrypted value while operating in isolated execution mode (column 15 line 61 – column 16 line 67).

England discloses an apparatus that uses an Operating System (OS) key to secure access to an operating system operating in a secure mode. Furthermore, England describes that “an unrelated operating system cannot gain access to the encrypted data” (column 17 lines 54-58) because of the requirement of the OS key.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim 1 wherein the key generator comprises:

a combiner to combine an identification of the OS nub and a master binding key (BK0) of the secure platform, the combined identification and the BK0 corresponding to the OSNK (column 12 line 53-65).

England discloses providing a one-way hashing function of the loaded components of the secure OS and then signing the hash with a private key corresponding to the operating system components.

Art Unit: 2131

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim 1 wherein the usage protector comprises:

an encryptor to encrypt the subset of the software environment using the OSNK, the encrypted subset being stored in a storage (column 7 lines 44- 50, column 13 lines 10-59); and

a decryptor to decrypt the encrypted subset using the OSNK, the encrypted subset being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim wherein the usage protector comprises:

an encryptor to encrypt a first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being stored in a storage (column 7 lines 44-50, column 13 lines 10-59);

a decryptor to decrypt the encrypted first hash value using the OSNK, the encrypted first hash value being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59); and

a comparator to compare the decrypted first hash value to a second hash value to generate a compared result, the compared result indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

Art Unit: 2131

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim 1 wherein the usage protector comprises:

a first encryptor to encrypt a first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being stored in a storage (column 7 lines 44-50, column 13 lines 10-59);

a second encryptor to encrypt a second hash value using the OSNK (column 7 lines 44-50, column 13 lines 10-59); and

a comparator to compare the encrypted second hash value to the encrypted first hash value to generate a compared result, the encrypted first hash value being retrieved from the storage, the compared result indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim 1 wherein the software environment comprises an operating system selected from the group consisting of a Windows operating system, a Windows 95 operating system, a Windows 98 operating system, a Windows NT operating system, and a Windows 2000 operating system (column 21 lines 25-29).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim 1 wherein the subset of the software environment is a registry of an operating system (column 13 lines 37 – 53).

Regarding claim 13, England discloses:

A method comprising:

generating an operating system nub key (OSNK) unique to an operating system (OS) nub, the OS nub being part of an operating system running on a secure platform; and

protecting usage of a subset of the software environment using the OSNK.

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, England discloses:

The method of claim 13 wherein generating the OSNK comprises:

combining an identification of the OS nub and a master binding key (BK0) of the secure platform, the combined identification and the BK0 corresponding to the OSNK (column 12 line 53-65).

Claim 16 is rejected as applied above in rejecting claim 13. Furthermore, England discloses:

The method of claim 13 wherein protecting usage comprises:

encrypting the subset of the software environment using the OSNK (column 7 lines 44- 50, column 13 lines 10-59);

storing the encrypted subset in a storage (column 7 lines 44- 50, column 13 lines 10-59); and

decrypting the encrypted subset from the storage using the OSNK (column 7 lines 44-50, column 13 lines 10-59).

Claim 17 is rejected as applied above in rejecting claim 13. Furthermore, England discloses:

The method of claim 13 wherein protecting usage comprises:

encrypting a first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being stored in a storage (column 7 lines 44-50, column 13 lines 10-59);

decrypting the encrypted first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59); and

comparing the decrypted first hash value to a second hash value to generate a compared result, the decrypted first hash value being retrieved from the storage, the compared result indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

Claim 18 is rejected as applied above in rejecting claim 13. Furthermore, England discloses:

The method of claim 13 wherein protecting usage comprises:

encrypting a first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being stored in a storage (column 7 lines 44-50, column 13 lines 10-59);

encrypting a second hash value using the OSNK (column 7 lines 44-50, column 13 lines 10-59); and

comparing the encrypted first hash value to the encrypted second hash value to generate a compared result, the encrypted first hash value being retrieved from the storage, the compared result indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

Claim 22 is rejected as applied above in rejecting claim 13. Furthermore, England discloses:

The method of claim 13 wherein the software environment comprises an operating system selected from the group consisting of a Windows operating system, a Windows 95 operating system, a Windows 98 operating system, a Windows NT operating system, and a Windows 2000 operating system (column 21 lines 25-29).

Claim 23 is rejected as applied above in rejecting claim 13. Furthermore, England discloses:

The method of claim 13 wherein the subset of the software environment is a registry of the operating system (column 13 lines 37 – 53).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, England discloses:

the computer program of claim 25 wherein the computer readable program code for generating the OSNK comprises:

computer readable program code for combining an identification of the OS nub and a master binding key (BK0) of the secure platform, the combined identification and the BK0 corresponding to the OSNK (column 12 line 53-65).

Claim 28 is rejected as applied above in rejecting claim 25. Furthermore, England discloses:

The computer program product of claim 25 wherein the computer readable program code for protecting usage comprises:

computer readable program code for encrypting the subset of the software environment using the OSNK (column 7 lines 44- 50, column 13 lines 10-59);

computer readable program code for storing the encrypted subset (column 7 lines 44- 50, column 13 lines 10-59); and

computer readable program code for decrypting the encrypted subset from the storage using the OSNK (column 7 lines 44-50, column 13 lines 10-59).

Claim 29 is rejected as applied above in rejecting claim 25. Furthermore, England discloses:

The computer program product of claim 25 wherein the computer readable program code for protecting usage comprises:

computer readable program code for encrypting a first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being stored in storage (column 7 lines 44-50, column 13 lines 10-59);

computer readable program code for decrypting the encrypted first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59); and

computer readable program code for comparing the decrypted first hash value to a second hash value to generate a compared result, the decrypted first hash value being retrieved from the storage, the compared result indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

Claim 30 is rejected as applied above in rejecting claim 25. Furthermore, England discloses:

The computer program product of claim 25 wherein the computer readable program code for protecting usage comprises:

computer readable program code for encrypting a first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being stored in storage (column 7 lines 44-50, column 13 lines 10-59);



computer readable program code for encrypting a second hash value using the OSNK (column 7 lines 44-50, column 13 lines 10-59); and

computer readable program code for comparing the encrypted first hash value to the encrypted second hash value to generate a compared result, the encrypted first hash value being retrieved from the storage , the compared result indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

Claim 34 is rejected as applied above in rejecting claim 25. Furthermore, England discloses:

The computer program product of claim 25 wherein the software environment comprises an operating system selected from the group consisting of a Windows operating system, a Windows 95 operating system, a Windows 98 operating system, a Windows NT operating system, and a Windows 2000 operating system (column 21 lines 25-29).

Claim 35 is rejected as applied above in rejecting claim 25. Furthermore England discloses:

The computer program product of claim 25 wherein the subset of the software environment is a registry of an operating system (column 13 lines 37 – 53).

Claim 38 is rejected as applied above in rejecting claim 37. Furthermore, England discloses:

The system of claim 37 wherein the key generator comprises:  
a combiner to combine an identification of the operating system nub and a master binding key (BK0) of the secure platform, the combined identification and BK0 corresponding to the OSNK (column 12 line 53-65).

Claim 40 is rejected as applied above in rejecting claim 37. Furthermore, England discloses:

The system of claim 37 wherein the usage protector comprises:  
an encryptor to encrypt the subset of the software environment using the OSNK, the encrypted subset being stored in a storage (column 7 lines 44- 50, column 13 lines 10-59); and  
a decryptor to decrypt the encrypted subset using the OSNK, the encrypted subset being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59).

Claim 41 is rejected as applied above in rejecting claim 37. Furthermore, England discloses:

The system of claim 37 wherein the usage protector comprises:  
an encryptor to encrypt a first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being stored in a storage (column 7 lines 44-50, column 13 lines 10-59);

a decryptor to decrypt the encrypted first hash value using the OSNK, the encrypted first hash value being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59); and

a comparator to compare the decrypted first hash value to a second hash value to generate a compared result, the compared result indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

Claim 42 is rejected as applied above in rejecting claim 37. Furthermore, England discloses:

The system of claim 37 wherein the usage protector comprises:

a first encryptor to encrypt a first hash value of the subset of the software environment using the OSNK, the encrypted first hash value being stored in a storage (column 7 lines 44-50, column 13 lines 10-59);

a second encryptor to encrypt a second hash value using the OSNK (column 7 lines 44-50, column 13 lines 10-59); and

a comparator to compare the encrypted second hash value to the encrypted first hash value to generate a compared result, the encrypted first hash value being retrieved from the storage, the compared result indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

Claim 46 is rejected as applied above in rejecting claim 37. Furthermore, England discloses:

The system of claim 37 wherein the software environment comprises an operating system selected from the group consisting of a Windows operating system, a Windows 95 operating system, a Windows 98 operating system, a Windows NT operating system, and a Windows 2000 operating system (column 21 lines 25-29).

Claim 47 is rejected as applied above in rejecting claim 37. Furthermore, England discloses:

The system of claim 37 wherein the subset of the software environment is a registry of an operating system (column 13 lines 37 – 53).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, England discloses:

The apparatus of claim 2 wherein the identification comprises a hash value of an item selected from the group consisting of the OS nub and a certificate representing the OS nub (column 12 line 53-65).

Claim 12 is rejected as applied above in rejecting claim 2. Furthermore, England discloses:

The apparatus of claim 2 wherein the BK0 is generated at random on a first invocation of a processor nub (column 17 lines 1-15).

Art Unit: 2131

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, England discloses:

The method of claim 14 wherein the identification comprises a hash value of an item selected from the group consisting of the OS nub and a certificate representing the OS nub (column 12 line 53-65).

Claim 24 is rejected as applied above in rejecting claim 14. Furthermore, England discloses:

The method of claim 14, wherein the BK0 is generated at random on a first invocation of a processor nub (column 17 lines 1-15).

Claim 27 is rejected as applied above in rejecting claim 26. Furthermore, England discloses:

The computer program product of claim 26 wherein the identification comprises a hash value of an item selected from the group consisting of the OS nub and a certificate representing the OS nub (column 12 line 53-65).

Claim 36 is rejected as applied above in rejecting claim 26. Furthermore, England discloses:

The computer program product of claim 26 wherein the BK0 is generated at random on a first invocation of a processor nub (column 17 lines 1-15).

Art Unit: 2131

Claim 39 is rejected as applied above in rejecting claim 38. Furthermore, England discloses:

The system of claim 38 wherein the identification comprises a hash value of an item selected from the group consisting of the OS nub and a certificate representing the OS nub (column 12 line 53-65).

Claim 48 is rejected as applied above in rejecting claim 38. Furthermore, England discloses:

The system of claim 38, wherein the BK0 is generated at random on a first invocation of a processor nub (column 17 lines 1-15).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 7-8, 19-20, 31-32, and 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over England et al. (U.S. Patent 6,327,652).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim 1 wherein the usage protector comprises:

a decryptor to decrypt a protected private key to generate a private key using the OSNK (column 7 lines 44-50, column 13 lines 10-59);

a signature generator coupled to the decryptor to generate a signature of the subset of the software environment using the private key, the signature being stored in a storage (column 7 lines 44-50, column 13 lines 10-59); and

a signature verifier to verify the signature to generate a modified/not modified flag using a public key, the signature being retrieved from the storage, the modified/not modified flag indicating whether the subset has been modified (column 7 lines 44-50, column 13 lines 10-59).

England discloses that a "CPU 140 is capable of performing cryptographic functions, such as signing, encrypting, decrypting, and authenticating." It is obvious that the capability exists in the apparatus of England to decrypt a protected private key. Also, it is described that the processor has the capability to generate signatures, and the verification procedure for a signature is analogous to the comparator of the one-way hash functions.

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim 1 wherein the usage protector comprises:

a manifest generator to generate a manifest of the subset of the software environment, the manifest describing the subset of the software environment, the manifest being stored in storage (column 7 lines 44-50, column 13 lines 10-59);

a signature generator coupled to the manifest generator coupled to the manifest generator to generate a manifest signature using a private key, the private key being decrypted by a decryptor using the OSNK, the manifest signature being stored in the storage (column 7 lines 44-50, column 13 lines 10-59);

a signature verifier to verify the manifest signature to generate a signature verified flag using a public key, the manifest signature being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59); and

a manifest verifier to verify the manifest to generate a manifest verified flag, the manifest being retrieved from the storage, the manifest verified flag and the signature verified flag being tested at a test center, the test center generating a pass/fail signal to indicate whether the subset has been modified (column 7 lines 44-50, column 13 lines 10-59).

A manifest is described as a "descriptor" or as "representing the subset in a concise manner." England discloses a representation of a component of code in an OS, "the identity is a cryptographic digest of the code for the component, or a well-known name, or any other string that is uniquely associated with the component." This can be interpreted as a "manifest" and the system of producing it as a "manifest generator." England discloses that a "CPU 140 is capable of performing cryptographic functions,



such as signing, encrypting, decrypting, and authenticating.” Also, England discloses “appending the identity of each loaded component” and “signing the boot log to attest to its validity.” The signing of the boot log represents a signature generator that is present, and a verifier to verify the validity of the signed component. Also, the manifest verifier is encompassed in the verification that the “boot log has not been tampered with” by comparing the cryptographic digests of the manifest created for each of the components.

Claim 19 is rejected as applied above in rejecting claim 13. Furthermore, England discloses:

The method of claim 13 wherein protecting usage comprises:

decrypting a protected private key to generate a private key using the OSNK (column 7 lines 44-50, column 13 lines 10-59);

generating a signature of the subset of the software environment using the private key, the signature being stored in a storage (column 7 lines 44-50, column 13 lines 10-59); and

verifying the signature to generate a modified/not modified flag using a public key, the signature being retrieved from the storage, the modified/ not modified flag indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

England discloses that a "CPU 140 is capable of performing cryptographic functions, such as signing, encrypting, decrypting, and authenticating." It is obvious that the capability exists in the apparatus of England to decrypt a protected private key. Also, it is described that the processor has the capability to generate signatures, and the verification procedure for a signature is analogous to the comparator of the one-way hash functions.

Claim 20 is rejected as applied above in rejecting claim 13. Furthermore, England discloses:

The method of claim 13 wherein detecting comprises:

generating a manifest of the subset of the software environment, the manifest describing the subset of the software environment, the manifest being stored in a storage (column 7 lines 44-50, column 13 lines 10-59);

generating a manifest signature of the manifest using a private key, the private key being decrypted using the OSNK, the manifest signature being stored in the storage (column 7 lines 44-50, column 13 lines 10-59);

verifying the manifest signature to generate a signature verified flag using a public key, the manifest signature being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59); and

verifying the manifest to generate a manifest verified flag, the manifest being retrieved from the storage, the manifest verified flag and the signature verified flag being tested at a test center, the test center generating a pass/fail signal, the pass/fail signal

indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

A manifest is described as a "descriptor" or as "representing the subset in a concise manner." England discloses a representation of a component of code in an OS, "the identity is a cryptographic digest of the code for the component, or a well-known name, or any other sting that is uniquely associated with the component." This can be interpreted as a "manifest" and the system of producing it as a "manifest generator." England discloses that a "CPU 140 is capable of performing cryptographic functions, such as signing, encrypting, decrypting, and authenticating." Also, England discloses "appending the identity of each loaded component" and "signing the boot log to attest to its validity." The signing of the boot log represents a signature generator that is present, and a verifier to verify the validity of the signed component. Also, the manifest verifier is encompassed in the verification that the "boot log has not been tampered with" by comparing the cryptographic digests of the manifest created for each of the components.

Claim 31 is rejected as applied above in rejecting claim 25. Furthermore, England discloses:

The computer program product of claim 25 wherein the computer readable program code for protecting usage comprises:

computer readable program code for decrypting a protected private key to generate a private key using the OSNK (column 7 lines 44-50, column 13 lines 10-59);

computer readable program code for generating a signature of the subset of the software environment using the private key, the signature being stored in a storage (column 7 lines 44-50, column 13 lines 10-59); and

computer readable program code for verifying the signature to generate a modified/not modified flag using a public key, the signature being retrieved from the storage, the modified/not modified flag indicating whether the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

England discloses that a "CPU 140 is capable of performing cryptographic functions, such as signing, encrypting, decrypting, and authenticating." It is obvious that the capability exists in the apparatus of England to decrypt a protected private key. Also, it is described that the processor has the capability to generate signatures, and the verification procedure for a signature is analogous to the comparator of the one-way hash functions.

Claim 32 is rejected as applied above in rejecting claim 25. Furthermore, England discloses:

The computer program product of claim 25 wherein the computer readable program code for protecting usage comprises:

computer readable program code for generating a manifest of the subset of the software environment, the manifest being stored in a storage (column 7 lines 44-50, column 13 lines 10-59);

computer readable program code for generating a manifest signature of the manifest using a private key, the private key being decrypted using the OSNK, the manifest signature being stored in the storage (column 7 lines 44-50, column 13 lines 10-59);

computer readable program code for verifying the manifest signature to generate a signature verified flag using a public key, the manifest signature being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59); and

computer readable program code for verifying the manifest to generate a manifest verified flag, the manifest being retrieved from the storage, the manifest verified flag and the signature verified flag being tested at a test center, the test center generating a pass/fail signal, the pass/fail signal indicating whether the subset of the software environment has been modified (column 7 lines 44-50, column 13 lines 10-59).

A manifest is described as a "descriptor" or as "representing the subset in a concise manner." England discloses a representation of a component of code in an OS, "the identity is a cryptographic digest of the code for the component, or a well-known name, or any other string that is uniquely associated with the component." This can be interpreted as a "manifest" and the system of producing it as a "manifest generator." England discloses that a "CPU 140 is capable of performing cryptographic functions,

Art Unit: 2131

such as signing, encrypting, decrypting, and authenticating.” Also, England discloses “appending the identity of each loaded component” and “signing the boot log to attest to its validity.” The signing of the boot log represents a signature generator that is present, and a verifier to verify the validity of the signed component. Also, the manifest verifier is encompassed in the verification that the “boot log has not been tampered with” by comparing the cryptographic digests of the manifest created for each of the components.

Claim 43 is rejected as applied above in rejecting claim 37. Furthermore, England discloses:

The system of claim 37 wherein the usage protector comprises:

a decryptor to decrypt a protected private key to generate a private key using the OSNK (column 7 lines 44-50, column 13 lines 10-59);

a signature generator coupled to the decryptor to generate a signature of the subset of the software environment using the private key, the signature being stored in a storage (column 7 lines 44-50, column 13 lines 10-59); and

a signature verifier to verify the signature to generate a modified/not modified flag using a public key, the signature being retrieved from the storage, the modified/not modified flag indicating whether the subset has been modified (column 7 lines 44-50, column 13 lines 10-59).

Art Unit: 2131

England discloses that a "CPU 140 is capable of performing cryptographic functions, such as signing, encrypting, decrypting, and authenticating." It is obvious that the capability exists in the apparatus of England to decrypt a protected private key. Also, it is described that the processor has the capability to generate signatures, and the verification procedure for a signature is analogous to the comparator of the one-way hash functions.

Claim 44 is rejected as applied above in rejecting claim 37. Furthermore England discloses:

The system of claim 37 wherein the usage protector comprises:

a manifest generator to generate a manifest of the subset of the software environment, the manifest describing the subset of the software environment, the manifest being stored in storage (column 7 lines 44-50, column 13 lines 10-59);

a signature generator coupled to the manifest generator coupled to the manifest generator to generate a manifest signature using a private key, the private key being decrypted by a decryptor using the OSNK, the manifest signature being stored in the storage (column 7 lines 44-50, column 13 lines 10-59);

a signature verifier to verify the manifest signature to generate a signature verified flag using a public key, the manifest signature being retrieved from the storage (column 7 lines 44-50, column 13 lines 10-59); and

a manifest verifier to verify the manifest to generate a manifest verified flag, the manifest being retrieved from the storage, the manifest verified flag and the signature

verified flag being tested at a test center, the test center generating a pass/fail signal to indicate whether the subset has been modified (column 7 lines 44-50, column 13 lines 10-59).

A manifest is described as a "descriptor" or as "representing the subset in a concise manner." England discloses a representation of a component of code in an OS, "the identity is a cryptographic digest of the code for the component, or a well-known name, or any other sting that is uniquely associated with the component." This can be interpreted as a "manifest" and the system of producing it as a "manifest generator." England discloses that a "CPU 140 is capable of performing cryptographic functions, such as signing, encrypting, decrypting, and authenticating." Also, England discloses "appending the identity of each loaded component" and "signing the boot log to attest to its validity." The signing of the boot log represents a signature generator that is present, and a verifier to verify the validity of the signed component. Also, the manifest verifier is encompassed in the verification that the "boot log has not been tampered with" by comparing the cryptographic digests of the manifest created for each of the components.



***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA  
12/20/04

  
EMMANUEL L. MOISE  
PRIMARY EXAMINER